符号理論の一般化について(代数的コード理論および語の組合せ論)

AUTHOR(S):

今井, 潤

CITATION:

今井, 潤. 符号理論の一般化について(代数的コード理論および語の組合せ論). 数理解析研究所講究録 1992, 786: 15-21

ISSUE DATE:

1992-06

URL:

http://hdl.handle.net/2433/82592

数理解析研究所講究録
第 786 巻 1992 年 15-21

符号理論の一般化について

今井 潤
NTT コミュニケーション科学研究所
NTT Communication Science Laboratories

概要

線形誤り訂正符号は、(準) 同型写像の誤りを検出する能力のある群とみることにより、より一般的な枠組で議論することができる。すなわち情報が、ある集合 (今の場合は群) によって表現されている時、その自己準同型写像を伝送路と思うことによって、伝送誤りを写像の誤りとして捉えることができる。本研究では、訂正能力を持つ符号を、任意の群の拡大 (短完全系列) として定義し、誤りの検出 (復号の原理) をホモロジー代数の範囲内で与えることを目的とする。同時にこの一般化が、無意味なものではなく、ある理想的な条件を満足するようになされたものであり、この一般化の結果としていくつかの重要な性質が得られる事についても述べる。

1 序：符号理論の第一基本原理

まず最初に議論するのは、与えられた条件を満足する符号を構成するのに必要な指導的原理と、その結果得られた符号あるいは符号族の持つ情報の所在をしめす基本定理である。

Theorem 1.1 (第一基本原理) $\mathcal{G}$;*the category of codes,* $\mathcal{X}$;*the subcategory of covering spaces with covering transformation group (or the subcategory of principal bundle)* とする。この時つぎの *1., 2., 3., 4.* の性質を満たす対応 $F:\mathcal{G}\longrightarrow\mathcal{X}$,$G:\mathcal{X}\longrightarrow\mathcal{G}$ が存在する。

1. $G\in Ob(\mathcal{G})$ に対して、

$$F(G):\tilde{X}\longrightarrow X;\textit{(the covering space with some transformation group } G')$$

such that: $\tilde{X}$;*connected*
$F(G)_*(\pi_1(\tilde{X}))$; *normal in* $\pi_1(X)$
$\pi_1(X)/\pi_1(\tilde{X})\cong G'$
G' は $\tilde{X}$ 上に自由に作用する。 *(acts freely on* $\tilde{X}$*)*
G' は G の *Cokernel*

2. $Y\in Ob(\mathcal{X})$ に対して、その *base space* を X とするとき $G(Y)$;*code such that*

$$[X,BG(Y)]\approx Hom(\pi_1(X),G(Y))\ (bijective)$$

3.

$$G(F(G))=G,\ F(G(Y))=Y\quad for\ any\ G\in Ob(\mathcal{G})\ and\ Y\in Ob(\mathcal{X})$$

4. 任意の $G\in Ob(\mathcal{G})$ に対し、ある F が存在し、コホモロジー環 $H^*(Btrans.group(F(G)),\mathcal{F})$ が符号 $G\in Ob(\mathcal{G})$ のすべての情報を含む。但し、$\mathcal{F}$ は適当な群あるいは、局所係数、または層を意味するものとする。

この定理は従来の符号の概念、従来の符号のカテゴリーでは定義もできないし、かつ理解不能である。この研究の目標は、この定理が成立するように、 符号の概念を、従来の符号の概念をふまえて一般化し、その結果として符号の構成や、復号、そして符号の持っている性能の分析を明解に行なえるようにすることにある。従って現時点ではこの定理の主張は単なる理想に過ぎないが、後に続くセクションで、符号概念を一般化し、その結果として、ここに書か

れた主張が完全ではないが、満たされる事を確認していくことになる。しかし、その主張すべてに対し厳密な証明は現時点では、残念ながら与えることはできない。そうはいっても、かなり良いところまで、確認することができるので、近い将来この定理1が正真正銘の定理になることができると筆者は考えている。なおこの研究において、符号理論の第二基本定理と呼ばれる主張は、後に述べるように、復号の原理に関するものである。

2 拡張された符号の定義

従来符号理論で扱われる有限集合としては、有限体上の vector space を考えることが多かった。これは計算機で扱われる情報の表現形式の制約と、初期の符号が多項式の理論と密接に関係しており、ガロア理論の要制からも有限体は非常に好都合であったという理由が考えられる。しかし、従来の概念では、符号のカテゴリーのオブジェクトが少な過ぎて、第一基本原理が成立しない。そこで、ここでは種々の制約を排し、一般化する。一般化された符号のカテゴリーは従来の符号は勿論包含しており、なおかつ、基本原理が成立するのにじゅうぶんなだけの豊富なオブジェクトを持っている。その結果、従来は複雑すぎて考慮されなかったようなものも考察の対象に入れることができる。実用的な観点からいうと条件にあう集合を可能な限り広い母体から探し、あとでその表現を状況に応じて変えるという方法を採ることが可能となる。

Definition 2.1 (ordinary code) $K := F_q$;有限体、$q := p^m(p : prime), etc$
いま情報が、K 上の *vector space* V の要素で表現されているものとする。伝送路を $f : V \longrightarrow V$ で表すと、これは誤りに対して無力である。そこで、*vector space* の一つの点を情報とするのではなくていくつかの点に一つの情報を表現させる（しかも均一に）と多少の誤りを許容できるようになる。ここで、多少という表現はいわゆる最小距離の範囲内の誤りを指している。
つまり、情報を $V \cong K^n$ の一点 x ではなく、

$$x + K^l \in K^{n+l}/K^l \cong K^n$$

に対応させると冗長な K^l だけの誤りを許容できるようになる。この状況は次のような *short exact sequence* で表すことができる。

$$0 \longrightarrow K^l \xrightarrow{\varphi} K^{n+l} \xrightarrow{\psi} K^n \longrightarrow 0\ (exact)$$

ここで、この系列に現れる単射を φ, 全射を ψ とし、適当な基底に対するその行列表示をそれぞれ G, H とするとき、H を *parity check matrix* と呼び、また、G を符号の *generator matrix* と呼ぶ。

上の定義から、符号とは、一つの coset に一つの情報を対応させることにより、$f : W/V \longrightarrow W/V$, where V is a subspace of W , e:error vector とするとき、

$$if\ e \in V\ then\ [f([x])] + e \sim [f([x])]$$

なる関係を用いて誤りの発生に対処することのできる情報の表現法であることがわかる。以上のことから容易に次のような定義の拡張ができる。

Definition 2.2 (extended code by 1-fold extension (abelian case)) Λ;*an arbitrary ring with unit* M_1, M_2, M_3;$\Lambda-$*modules,* この時 、$Ext^1_\Lambda(M_3, M_1)$ の元すなわち、

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0\ (exact)$$

の同値類を拡張された第一種符号という。

この定義は、従来の符号は

$$Ext^1_\Lambda(M_3, M_1) \cong Ext^1_K(M_3, M_1) \cong 0$$

であるから、M_3 と M_1 から唯一決まっていたのに対し、拡張された符号では、M_3 と M_1 のみでは決定できないし、M_3 と M_1 をもちいて、作られる符号全体は、Baer sum によって群をなす。このことから、この符号は、既知の符号から、簡単な演算によって新しい符号を合成することができることがわかる。

Definition 2.3 (extended code by group extension (non abelian case with abelian kernel)) G;*a group,* A;*a left* G-*module,* とする。このとき、$Ext^2_{ZG}(Z, A) \cong H^2(G, A)$ の元すなわち、

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1\ (exact)$$

の同値類を拡張された第二種符号という。

Definition 2.4 (ex.code by group extension (non abelian case with non abelian kernel)) N, E, G : *groups*, C; *the center of* N とするとき、

$$1 \longrightarrow N \longrightarrow E \longrightarrow G \longrightarrow 1 \ (exact)$$

の同値類を拡張された第三種符号という。このとき、この同値類の集合を $\mathcal{E}(G,N)$ とおく時、以下が成立している。
(1)$\mathcal{E}(G,N) \neq \phi$ *if and only if some obstruction* $\in H^3(G,C)$ *is zero*
(2)$\mathcal{E}(G,C) \approx H^2(G,C)$ *(bijective) if* $\mathcal{E}(G,C) \neq \phi$

(Remark 1) 2つの拡張された符号が同値であるとは、

$$1 \longrightarrow N \longrightarrow E \longrightarrow G \longrightarrow 1 \ (exact), 1 \longrightarrow N \longrightarrow E' \longrightarrow G \longrightarrow 1 \ (exact)$$

にたいして、isomorphism:$E \longrightarrow E'$ が存在して以下の図式が可換となることである。

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

(Remark 2) 以上の定義は群の拡大の理論に沿って符号を特徴づけたものである。ここで、注目すべきことは、すべての種の符号があるコホモロジー群と対応づけられていることである。群の拡大の理論は群のコホモロジー理論と等価であるから、この事は当然ではあるが、我々はこの事実を利用し、符号が幾何学的なコホモロジーによって、特徴付けられることを主張し、示したいのである。この部分の主張が、定理1（実は予想に近い）の4番目の主張である。

Definition 2.5 (structurizable) 第二種符号

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1 \ (exact)$$

が構造化可能 *(structurizable)* であるとは、上の完全系列が 分裂 *(split)* することを指す。すなわち準同型写像 s : $G \longrightarrow E$ *such that* $\pi s = id_G$ が存在することと同値であり、さらに次の符号と上の符号が同値になる事とも言い替えられる。

$$0 \longrightarrow A \xrightarrow{i'} A \bowtie G \xrightarrow{\pi'} G \longrightarrow 1 \ (exact)$$

この形の符号は、ある意味で、標準的な役割を持つ。通常の符号の世界でも、組織化符号 *(systematic code)* なる概念があり、情報部分と検査部分に基底が分離できる状況を指している。この状況は実用的な意味でも都合の良いものであり、拡張された符号でもこの状況を一つの目安として考えることが重要である。

3 符号理論の第二基本原理

この節では拡張された符号に対して、復号法が存在することを述べる。この事実を第二基本原理と呼び、拡張された符号が誤りの検出の意味でも従来の符号の拡張になっていることを主張する重要な定理である。定理を述べるまえに、先ず拡張された符号に対する誤りの概念を明確にしておく。

Definition 3.1 (definition of error) 拡張された符号 G;

$$G := N \longrightarrow \Pi \longrightarrow \Pi/N \ (exact)$$

に対して、自己同型写像 $\varphi : G \longrightarrow G$ があるとき、φ から誘導される Π 上の自己同型写像が存在するが、（記号を混用して、この写像も φ と書くことにする）このとき、Π のある部分集合 Δ があって、φ が Δ 上で同型写像にならない時に、$\varphi(\Delta)$ を φ の誤りという。
つまり、本研究では、符号の概念のみならず、誤りの概念も拡張し、部分集合の間の対応の異変をも誤りとして取り扱うことにする。

Theorem 3.1 (第二基本原理) 拡張された符号 G;

$$G := N \longrightarrow \Pi \longrightarrow \Pi/N \ (exact)$$

の誤りを持つ自己同型写像 φ に対して、φ から G の *Cokernel* $(:= \Pi/N)$ 上に誘導される写像が同型であり、かつ $H^*(\Pi)$(*or* $H_*(\Pi)$) に関する情報が既知であれば、φ の誤りを検出することができる。

Proof: 一般的な枠組内で証明することもできるが、長くなるので、ここでは、具体例として特にΠが有限生成アーベル群の場合を例にとって説明をする。この場合には、局所的な同型性の乱れが、生成元の個数に着目することによって発見できる。この手法は有限生成アーベル群に限らず、一般的な群にも有効な手段であるので、この方法をGenerator Counting Method と呼ぶことにする。

1. Πがn個の位数d(素数とする）の有限巡回群の直和に同型である場合
いま、次の情報が既知であるとする。

$$Order(H_2(\Pi, \mathrm{Z})) = d^{n(n-1)/2}$$

符号Gを

$$G := N \longrightarrow \Pi \longrightarrow \Pi/N \ (exact),\ \Pi/N := \text{cyclic of order d}$$

となるように選び、$\varphi(\Pi/N)$;isomorphic, $\varphi(N)$;not isomorphic と仮定した時に spectral sequence を調べることによって、$\varphi(N)$ に誤り（生成元の数の変化）があることが導かれることを示す。この場合には符号Gに対して、ホモロジーの Lyndon-Hochschild-Serre spectral sequence を用いる。
先ずΠが次のような表示 (Generators and Relaions)

$$\Pi = (x_1, x_2, ..., x_n \mid x_1^d, ..., x_n^d, [x_i, x_j], i < j) =: (F, R)$$

を持つ事と、群のホモロジーに関する結果から、

$$H_2(\Pi, \mathrm{Z}) \cong F'/[R, F] \cong K' \text{ where } K = F/[R, F],\ K' \text{ is commutator subgroup of K}$$

が得られ、さらに$a_i = x_i[R, F]$とおくと

$$K' =< [a_i, a_j],\ (\ i < j\ )\ >,\ [a_i, a_j] \in Z(K),\ a_j^d \in Z(K)$$

が導ける。これより

$$a_j^d = a_i a_j^d a_i^{-1} = (a_i a_j a_i^{-1})^d = ([a_i, a_j] a_j)^d = [a_i, a_j]^d a_j^d$$

従って$[a_i, a_j]^d = 0\ (i < j)$が解り、$dH_2(\Pi, \mathrm{Z}) = 0$が得られる。
今、仮定として、φによって、Nが同型でない群に写されたとする。例えば

$$\varphi(N) \cong \coprod_m \mathrm{Z}_d \text{ where } n - m > 1$$

と仮定する。以下の議論では、φが同型であると仮定すると矛盾が導かれることを示し、その結果、$\varphi(\Pi/N)$が同型であるという前提条件より、$\varphi(N)$の異常が検出できることを述べる。
$\varphi(G)$に対して L-H-S spectral sequence を適用する。その結果得られる情報は以下のようなものである。

$$E^2_{p,q} = H_p(\Pi/N, H_q(\varphi(N), \mathrm{Z})) \Longrightarrow H_{p+q}(\Pi, \mathrm{Z})$$

Π/Nが有限巡回群であるから、巡回群のホモロジーの計算結果より、

$$E^2_{2,0} = H_2(\Pi/N, H_0(\varphi(N), \mathrm{Z})) = 0 = E^\infty_{2,0}$$

したがって、$H_2(\Pi, \mathrm{Z})$ の filtration は、

$$0 = \Phi^{-1}H_2 \subset \Phi^0 H_2 \subset \Phi^1 H_2 = \Phi^2 H_2 = H_2,\ \Phi^0 H_2/\Phi^{-1} \cong E^\infty_{0,2},\ \Phi^1 H_2/\Phi^0 H_2 \cong E^\infty_{1,1}$$

また$E^2 - term$を調べることにより、$E^2_{0,2} \cong E^\infty_{0,2},\ E^2_{1,1} \cong E^\infty_{1,1}$ なる情報が得られる。ゆえに次の完全系列が得られる。

$$0 \longrightarrow E^2_{0,2} \longrightarrow H_2(\Pi, \mathrm{Z}) \longrightarrow E^2_{1,1} \longrightarrow 0$$

そして、冒頭の議論より、$H_2(\Pi, \mathrm{Z})$は体Z_d上の線形空間となるので、上記の完全系列は分裂し、

$$H_2(\Pi, \mathrm{Z}) \cong E^2_{0,2} \bigoplus E^2_{1,1} \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

となる。あとは機械的な計算により以下の事項を確認することができる。

$$H_1(\varphi(N),\mathrm{Z}) \cong \varphi(N)/\varphi(N)' \cong \varphi(N) \cong \coprod_m \mathrm{Z}_d$$

$$E^2_{1,1} = H_1(\Pi/N, H_1(\varphi(N),\mathrm{Z})) \cong \coprod_m H_1(\Pi/N,\mathrm{Z}_d) \cong \coprod_m \mathrm{Z}_d$$

$$E^2_{0,2} = H_0(\Pi/N, H_2(\varphi(N),\mathrm{Z})) \cong H_2(\varphi(N),\mathrm{Z})$$

以上の情報から、上の (1) 式の両辺の次元を計算すれば矛盾が導かれる。

2. Π が階数 k の自由アーベル群の場合
いま、次の情報が既知であるとする。

$$rank(H^n(\Pi,\mathrm{Z})) = \begin{pmatrix} k \\ n \end{pmatrix} \text{ if } k \geq n$$

符号 G を

$$G := N \longrightarrow \Pi \longrightarrow \Pi/N \ (exact),\ \Pi/N \cong \mathrm{Z}$$

となるように選ぶ。仮定として、φ によって、N が同型でない群に写されたとする。例えば、

$$rank(\varphi(N)) = k - d,\ d \geq 2$$

と仮定する。以下の議論では、（1）と同様にして、φ が同型であると仮定すると矛盾が導かれることを示し、その結果、$\varphi(\Pi/N)$ が同型であるという前提条件より、$\varphi(N)$ の異常が検出できることを述べる。
$\varphi(G)$ に対して L-H-S spectral sequence を適用する。

$$E_2^{p,q} = H^p(\Pi/N, H^q(\varphi(N),\mathrm{Z})) \Longrightarrow H^{p+q}(\Pi,\mathrm{Z})$$

いま $\Pi/N \cong \mathrm{Z}$ より、$E_2^{p,q} = 0$ if $p \neq 0,1$ だから $E_2 - term$ には自明でない群は $p = 0,1$ なる 2 本の直線上にのみ存在する。従って、次の完全系列が存在する。

$$0 \longrightarrow E_2^{1,n-1} \longrightarrow H^n(\Pi,\mathrm{Z}) \longrightarrow E_2^{0,2} \longrightarrow 0$$

以下、上の完全系列の両端を評価して、中央と比較することによって矛盾を導く。$H^{n-1}(\varphi(N),\mathrm{Z})$ が $\Pi/N - trivial$ であることに注意すると、両端の $E_2 - term$ は以下のように計算される。

$$E_2^{1,n-1} = H^1(\Pi/N, H^{n-1}(\varphi(N),\mathrm{Z})) \cong Hom(\mathrm{Z}, H^{n-1}(\varphi(N),\mathrm{Z})) \cong H^{n-1}(\varphi(N),\mathrm{Z})$$

$$E_2^{0,n} = H^0(\Pi/N, H^n(\varphi(N),\mathrm{Z})) \cong H^n(\varphi(N),\mathrm{Z})$$

従って、

$$rank(E_2^{1,n-1}) + rank(E_2^{0,n}) = \begin{pmatrix} k-d \\ n \end{pmatrix} \neq rank(H^n(\Pi,\mathrm{Z}))$$

よって矛盾が導かれた。

3. Π が自由アーベル群と有限位数アーベル群を共に含み、Π/N が自由アーベル群、N が torsion part である場合
この場合には N の位数 n を知っているだけで、Π/N の元に情報を対応させて伝える時に、誤りの訂正ができる。つまり、φ は Π/N 上の同型を誘導しているという仮定より、$a \in \Pi$ に対して、$\varphi(a)$ の値は、N の元の差を無視すれば正しい。ここに出現した N の元が誤りに相当するものだから、これを除去できるアルゴリズムがあればすなわち誤りを訂正できると言うことができる。この元を除去するには、$\varphi(a)$ を n 倍して、さらに n で割れば良い。なぜなら、N は有限位数だからである。

(Remark) 上記の事例 1、2、では N を比較的大きいものにとっているが、これは spectral sequence の $E_2 - term$ の計算を楽にするための細工である。Π/N をもう少し大きくとってやると、$E_2 - term$ の計算のために自明でない群のコホモロジーの情報が必要になって計算手数が増大するだけである。

4 応用

4.1 Mordell-Weil lattice 理論

Definition 4.1 *(Mordell-Weil gourp)*
*K;*体 *(char* $\neq 2,3$*)*
K 上の楕円曲線　E/K とは，次のような標準的な方程式で定義される代数曲線である．

$$y^2 = x^3 + Ax + B, (A, B \in K, 4A^3 + 27B^2 \neq 0)$$

また

$$E(K) := \{P = (x, y) \in E \mid x, y \in K\} \cup O, where\ O = \infty$$

を E の K ー有理点と呼ぶ．*E(K)* は O を単位元とするアーベル群の構造を持つ．この群を *Mordell-Weil* 群と呼ぶ。また $E(K)_{tor}$ を *E(K)* のねじれ部分群と呼ぶ。

Definition 4.2 （代数的サイクル）
代数多様体 X の（余次元 d の）既約部分多様体 Z_i の整係数一次結合 $Z := \sum n_i Zi$ を，X 上の（余次元 d の）代数的サイクルという．それらの全体を $Z^d(X)$ と書く．また各 Z にそのコホモロジー類を対応させるサイクル写像 $\gamma : Z^d(X) \to H^{2d}(X)$ の像 $C^d(X)$ も代数的サイクルと呼ぶ．とくに，正標数において $H^{2d}(X) = C^d(X)$ となるとき，X は余次元 d で超特異的という．

さて代数的サイクル E(K) に適当な内積を定義して，この群を格子 (lattice) として考えようという研究が Mordell-Weil lattice の理論と呼ばれるものである。

Definition 4.3 (T.Shioda) *(Mordell-Weil lattice (MWL))*
紙数の関係で，正確な定義は原典にあたっていただくとして，ここでは定義のあらすじを述べるだけにとどめる．
定義体 $K = k(t)$; 体 k 上の 1 変数代数関数体とする．一般には K は，ある代数曲線 C/k の関数体 $k(C)$ でよい．
まず K 上の楕円曲線 E に対し，自然に構成される楕円曲面（小平ー *Néron model*）$f : S \to C$ を考え，その *Néron-Severi group* を *NS(S)* とする．この楕円曲面はそのファイバーをとれば，K 上の楕円曲線とみなすことができ，断面のなす群は *E(K)* と同型になる．いま T を，零断面 *(O)* とファイバーの規約成分全体で生成される *NS(S)* の部分群とするとき，$E(K) \cong NS(S)$ が成立する．そしてこの同型を用いて次のような準同型が一意的に定義できる．

$$\varphi : E(K) \to NS(S) \otimes Q,\ such\ that\ Im(\varphi) \perp T,\ \varphi(P) \equiv (P) mod T \otimes Q,\ Ker(\varphi) = E(K)_{tor}$$

但し，$P \in E(K)$ に対し，P に対応する断面を *(P)* と書いている．さて，代数曲面 S には，交点理論によって S 上の因子 D, D' に対し交点数 *(D.D')* が定義されこれが *NS(S)* 上に *bilinear pair* を誘導する．そこで，上記の写像 φ によって，$E(K)$ を *NS(S)* に埋め込むことによって $E(K)$ 上に *symmetric bilinear form* を交点数を用いて次のように定義する．

$$\langle P, P' \rangle := -(\varphi(P).\varphi(P'))$$

これを *height pairing* という．このとき，$E(K)/E(K)_{tor}$ は $\langle\ ,\ \rangle$ に関して　*positive lattice* になり，また，

$$E(K)^0 := \{P \in E(K); ((P)\Theta_{v,0}) = 1,\ for\ all\ reducible\ fiber\ and\ \Theta_{v,0}\ with\ (\Theta_{v,0}(O)) = 1\}$$

は $\langle\ ,\ \rangle$ に関して　*positive even integral lattice* となる．これらを各々 *Mordell-Weil lattice* および *narrow Mordell-Weil lattice* ($E(K)^0$ と書く) という．

4.2 MWL code

MWL を用いて、われわれは Modell-Weil group E(K) から拡張された符号をつくることができる。容易に分かるように MWL の定義より、次の完全系列が存在する。

$$0 \longrightarrow E(K)_{tor} \longrightarrow E(K) \longrightarrow E(K)/E(K)_{tor} \longrightarrow 0$$

そこで、前節の結果より、$E(K)/E(K)_{tor}$ を符号語とするような拡張された符号が定義できる。復号アルゴリズムが容易なことは前節でも述べたが、この符号で良い点は、楕円曲線を適当に選ぶことによって $(E(K)/E(K)_{tor}, <\ ,\ >)$ が、球体充填問題に対し、高密度の充填を可能にする格子を与えることである。このことは、同じ最小距離

を持ちながらより多くの情報を正確に伝えることのできる符号を作れる点で有利である。また従来、特定の次元で最密充填解を与えていることで良く知られた格子も楕円曲線を適当にとることによってMWLとして再定義することにより、符号として利用可能になる。
(例) [Shioda]
k を標数 $p>0$ の体で、有限体 F_{p^2} を含むものとする。このとき、

$$E:\ y^2=X^3+1+t^{p+1},\ \text{;elliptic curve over } K:=k(t) \text{ where } p\equiv -1(mod 6)$$

から定義されるMWLは高次元球体充填問題に対し、従来知られている解よりも高密度の充填を与える。

5 群作用を持つ幾何学的対象との対応 について

冒頭の基本原理で述べたように、群作用を持つ特殊な幾何学的対象との対応を完成させるために符号を一般化する必要があったのだが、現時点では、まだこの対応の候補となる対象は明確になっていない。研究の進展状況によってはこれらの基本原理を修正する必要があるかもしれないが、もし対応が確立されれば、符号理論にとって、それは有益であると考えられる。また、この対応は唯一通りしかないというものではないことも注意する必要がある。実際、現在研究中の対応は、2通りあり、一つは、非常に抽象的なsimplicial objectに基づいて構成される幾何学的対象との間の関係であり、これは第一基本原理の中の（4）にとって、都合の良い対応である。なぜなら構成的に作られた幾何学的対象のホモトピーやホモロジーは計算がし易くなっているからである。もう一つの方は、幾何学的構造は非常に簡単であり、作用している群の構造の方に重点の置かれている対象との間の対応である。こちらの方は、符号の群としての性質を組合せ論的に調べるのに都合の良い対応であり、また逆に、簡単な幾何学的対象を基にして、要求されている性質を満たすような符号を作ろうとする時には、この対応は非常に有利である。

参考文献

[1] Wood, J. A. *Spinor groups and algebraic coding theory*, Journal of Combinatorial Theory, Series A 1989.

[2] Shioda, T. *Mordell-Weil lattices and sphere packings*, American Journal of Mathematics vol 113, Number 5 1991 931-948.

[3] MacLane, S. *Homology*, Springer-Verlag,1963.

[4] Freed, D. S., Uhlenbeck, K. K. *Instantons and Four-manifolds*, Springer-Verlag 1984.